HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200312858-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): John APOSTOLOPOULOS et al.

Confirmation No.: 1717

Application No.: 10/698,784

Examiner: Devin E. Almeida

Filing Date: 10/31/2003

Group Art Unit: 2132

Title: A METHOD AND APPARATUS FOR ENSURING THE INTEGRITY OF DATA

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 09/30/2008.

☑ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $130	☐ 2nd Month $490	☐ 3rd Month $1110	☐ 4th Month $1730

☐ The extension fee has already been filed in this application.

☑ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $540. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

John APOSTOLOPOULOS et al.

By /John P. Wagner, Jr./

John P. Wagner, Jr.

Attorney/Agent for Applicant(s)

Reg No. : 35,398

Date : 12/01/2008

Telephone : 408-377-0500

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	APOSTOLOPOULOS et al.	Patent Application	
Application No.:	10/698,784	Group Art Unit:	2132
Filed:	October 31, 2003	Examiner:	Almeida, Devin E.

For: A METHOD AND APPARATUS FOR ENSURING THE INTEGRITY OF DATA

APPEAL BRIEF

Table of Contents

	Page
Real Party in Interest	1
Related Appeals and Interferences	2
Status of Claims	3
Status of Amendments	4
Summary of Claimed Subject Matter	5
Grounds of Rejection to Be Reviewed on Appeal	9
Argument	10
Conclusion	21
Appendix – Clean Copy of Claims on Appeal	22
Appendix – Evidence Appendix	29
Appendix – Related Proceedings Appendix	30

I. Real Party in Interest

The assignee of the present application is Hewlett-Packard Development Company, L.P.

II. Related Appeals and Interferences

A related appeal for Application No. 10/617,348 is currently pending before the Board of Patent Appeals and Interferences (Appeal Brief submitted August 18, 2008).

III. Status of Claims

Claims 1-34 are pending. Claims 1, 2, 5-15, 18-30 and 32-34 are rejected. Claims 3, 4, 16, 17 and 31 are objected to. This Appeal involves Claims 1, 2, 5-15, 18-30 and 32-34.

IV. Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Office Action mailed July 31, 2008, has not been filed.

V. Summary of Claimed Subject Matter

As recited in Claim 1, "[a] method for ensuring the integrity of data" is described. This embodiment is depicted at least in Figures 4A, 4B, 9, 10A and 10B. "Figure 10B illustrates the operation of an embodiment of the present invention where there are multiple segments within a plurality of packets and more than one cryptographic checksum is necessary to achieve the level of data integrity and security required" (page 35, lines 19-22). "[A] cryptographic checksum is calculated at 1015 for a plurality of first segments in a plurality of data packets" (page 35, line 23, through page 36, line 1). "Media stream 411 is separated, at 412, into segments, each comprising one or more independently decodable parts (A, B, etc). It is noted again that a packet payload can comprise one or more independently decodable parts or segments and, in some embodiments, the independently decodable parts can comprise independently truncatable units. As shown at packet 413, a cryptographic checksum is computed for each of the decodable parts or truncatable units, in order of priority" (page 17, lines 2-9). "The calculation and inclusion of the cryptographic checksum, it is noted, can occur at differing rates for different data segments and packets. This allows different data segments, in either the same data packet or in different data packets, to have different priorities or different integrity checking requirements" (page 33, lines 9-13). "At step 1025, the cryptographic checksum is included at 1025 in an additional packet" (page 36, lines 6-7).

As recited in Claim 14, "[a] computer readable medium having instructions stored therein for implementing a method for ensuring integrity of data" is described. This embodiment is depicted at least in Figures 4A, 4B, 9, 10A and 10B. "Figure 10B illustrates the operation of an embodiment of the present invention where there are multiple segments

within a plurality of packets and more than one cryptographic checksum is necessary to achieve the level of data integrity and security required" (page 35, lines 19-22). "[A] cryptographic checksum is calculated at 1015 for a plurality of first segments in a plurality of data packets" (page 35, line 23, through page 36, line 1). "Media stream 411 is separated, at 412, into segments, each comprising one or more independently decodable parts (A, B, etc). It is noted again that a packet payload can comprise one or more independently decodable parts or segments and, in some embodiments, the independently decodable parts can comprise independently truncatable units. As shown at packet 413, a cryptographic checksum is computed for each of the decodable parts or truncatable units, in order of priority" (page 17, lines 2-9). "The calculation and inclusion of the cryptographic checksum, it is noted, can occur at differing rates for different data segments and packets. This allows different data segments, in either the same data packet or in different data packets, to have different priorities or different integrity checking requirements" (page 33, lines 9-13). "At step 1025, the cryptographic checksum is included at 1025 in an additional packet" (page 36, lines 6-7).

As recited in Claim 23, "[a]n apparatus for ensuring the integrity of data" is described. This embodiment is depicted at least in Figures 4A, 4B and 9. "Figure 9 is a block diagram of an apparatus for calculating cryptographic checksums across packets in accordance with an embodiment of the present invention" (page 31, lines 13-15). "Apparatus 901 comprises a receiver 902 which receives data stream 920" (page 31, line 15-16). "Media stream 411 is separated, at 412, into segments, each comprising one or more independently decodable parts (A, B, etc). It is noted again that a packet payload can comprise one or more independently decodable parts or segments and, in some embodiments, the independently decodable parts can comprise independently truncatable units. As shown at packet 413, a cryptographic

checksum is computed for each of the decodable parts or truncatable units, in order of priority" (page 17, lines 2-9). "The calculation and inclusion of the cryptographic checksum, it is noted, can occur at differing rates for different data segments and packets. This allows different data segments, in either the same data packet or in different data packets, to have different priorities or different integrity checking requirements" (page 33, lines 9-13). "Cryptographic checksums are calculated by cryptographic checksum calculator 903 based on various criteria" (page 31, lines 16-18). "Apparatus 901 also includes a cryptographic checksum (CCS) appender 904 for appending or concatenating, or otherwise assembling, packets of cryptographic checksums and data segments" (page 31, lines 21-23).

As recited in Claim 27, "[a] method for ensuring the integrity of data" is described. This embodiment is depicted at least in Figures 9, 10A and 10B. "Figure 10B illustrates the operation of an embodiment of the present invention where there are multiple segments within a plurality of packets and more than one cryptographic checksum is necessary to achieve the level of data integrity and security required" (page 35, lines 19-22). "[A] cryptographic checksum is calculated at 1015 for a plurality of first segments in a plurality of data packets" (page 35, line 23, through page 36, line 1). "The calculation and inclusion of the cryptographic checksum, it is noted, can occur at differing rates for different data segments and packets. This allows different data segments, in either the same data packet or in different data packets, to have different priorities or different integrity checking requirements" (page 33, lines 9-13). "At step 1025, the cryptographic checksum is included at 1025 in an additional packet" (page 36, lines 6-7).

As recited in Claim 29, "[a] method for ensuring the integrity of data" is described. This embodiment is depicted at least in Figures 9, 10A and 10B. "Figure 10B illustrates the operation of an embodiment of the present invention where there are multiple segments within a plurality of packets and more than one cryptographic checksum is necessary to achieve the level of data integrity and security required" (page 35, lines 19-22). "The calculation and inclusion of the cryptographic checksum, it is noted, can occur at differing rates for different data segments and packets. This allows different data segments, in either the same data packet or in different data packets, to have different priorities or different integrity checking requirements" (page 33, lines 9-13). "[A] cryptographic checksum is calculated at 1015 for a plurality of first segments in a plurality of data packets" (page 35, line 23, through page 36, line 1). "At step 1025, the cryptographic checksum is included at 1025 in an additional packet" (page 36, lines 6-7).

As recited in Claim 32, "[a]n apparatus for verifying the integrity of data" is described. This embodiment is depicted at least in Figure 12. "Referring now to Figure 12, a schematic diagram of a receiver 1200 having an integral integrity check module 1202 is shown" (page 38, lines 3-5). "In operation, receiver 1200 receives potentially processed data packets, and the integrity check module 1202 checks the integrity of the packets by computing the cryptographic checksums for the received data packets (i.e. a new cryptographic checksum) and compares it to the received cryptographic checksums (e.g., previously determined cryptographic checksum)" (page 38, lines 5-11). "The calculation and inclusion of the cryptographic checksum, it is noted, can occur at differing rates for different data segments and packets. This allows different data segments, in either the same data packet or in different data packets, to have different priorities or different integrity checking requirements" (page 33, lines 9-13).

VI. Grounds of Rejection to Be Reviewed on Appeal

1. Claims 1, 14 and 23 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

2. Claims 1, 2, 5-10, 12, 13, 23-30 and 32-34 are rejected under 35 U.S.C. §103(a) as being over "Secure Scalable Video Streaming for Wireless Networks" by Wee et al., hereinafter referred to as "Wee," in view of U.S. Patent No. 5,958,080 by Kang, further in view of U.S. Patent No. 5,790,669 by Miller et al., hereinafter referred to as "Miller."

3. Claims 11, 14, 15 and 18-22 are rejected under 35 U.S.C. §103(a) as being over Wee in view of Kang, further in view of Miller, yet further in view of U.S. Patent Application Publication No. 2002/0095586 by Doyle et al., hereinafter referred to as "Doyle."

VII. Argument

1. Whether Claims 1, 14 and 23 are properly rejected under 35 U.S.C. §112, second paragraph.

The Final Office Action mailed July 31, 2008, hereinafter referred to as the "instant Office Action," states that Claims 1, 14 and 23 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, it is asserted that it is unclear as to whether the data packets of the plurality of data packets have a first data segment or a plurality of first data segments and whether the data packets of the plurality of data packets have a second data segment or a plurality of second data segments.

Applicants respectfully submit that the claimed embodiments reciting "a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments" satisfy the requirements of 35 U.S.C. §112, second paragraph. The instant specification provides additional support for the definiteness of the claimed embodiments, for example, at least at page 36, line 23, through page 37, line 1).

Moreover, Applicants agree that the claims can be interpreted as indicated in the instant Office Action, but respectfully submit that they are not limited to such an interpretation, while still satisfying the requirements of 35 U.S.C. §112, second paragraph.

2. Whether Claims 1, 2, 5-10, 12, 13, 23-30 and 32-34 are unpatentable under 35 U.S.C. §103(a) by Wee in view of Kang, further in view of Miller.

The instant Office Action states that Claims 1, 2, 5-10, 12, 13, 23-30 and 32-34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wee in view of Kang, further in view of Miller. The Applicants have reviewed Wee, Kang and Miller and respectfully submit

that the embodiments recited in Claims 1, 2, 5-10, 12, 13, 23-30 and 32-34 are patentable over the combination of Wee, Kang and Miller, for at least the following rationale.

Applicants respectfully direct the Examiner to independent Claim 1 that recites that an embodiment of the present invention is directed to (emphasis added):

> A method for ensuring the integrity of data, comprising:
> a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums, wherein said plurality of first data segments have a different priority than said plurality of second data segments; and
> enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

Independent Claims 23, 27, 29 and 32 include similar recitations. Claims 2, 5-10, 12 and 13 that depend from independent Claim 1, Claims 24-26 that depend from independent Claim 23, Claim 28 that depends from independent Claim 27, Claim 30 that depends from independent Claim 29, and Claims 33 and 34 that depend from independent Claim 32 also include these recitations.

"As reiterated by the Supreme Court in *KSR*, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries" including "[a]scertaining the differences between the claimed invention and the prior art" (MPEP 2141(II)). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious"

(emphasis in original; MPEP 2141.02(I)). Applicants note that "[t]he prior art reference (or references when combined) need not teach or suggest all the claim limitations, however, Office personnel must explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art" (emphasis added; MPEP 2141(III)).

Applicants note that the instant Office Action recites that "Wee does not disclose calculating a cryptographic checksum for said plurality of first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums" (instant Office Action; page 4, lines 3-5). Applicants understand the instant Office Action to rely on Kang and Miller as overcoming this deficiency.

Applicants respectfully note that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention" (emphasis in original; MPEP 2141.02(VI); *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984)).

First, Applicants respectfully submit that Kang teaches away from "enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets" (emphasis added) as claimed.

As understood by Applicants, Kang discloses (emphasis added; col. 6, lines 16-27)

> a method of detecting errors in an operation of loading information from an upper processor in a digital cellular system base station, wherein the information is divided into a plurality of packets, comprises the steps of receiving header information at an early stage of the operation, wherein the

header information indicates a sent packet count corresponding to the number of packets in the plurality of packets; calculating for each packet a packet checksum corresponding to the packet; including in each packet the packet checksum corresponding to the packet and a packet sequence number corresponding to the position of the packet in the information

Moreover, Kang recites that "[i]n any case, the upper processor computes a packet checksum for each packet and includes it in the packet" (emphasis added; col. 8, lines 32-34). Accordingly, Applicants respectfully submit that Kang discloses that packet checksums for each packet are included in each packet. In particular, by disclosing that a packet checksum for each packet is included in each packet, Applicants respectfully submit that Kang teaches away from "enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets" (emphasis added) as claimed.

Applicants note that Kang does disclose "calculating a total checksum by summing all of the packet checksums" (col. 6, lines 28-29). However, Applicants respectfully submit that a total checksum is not "said cryptographic checksums for said plurality of said first data segments" as claimed. For instance, Applicants respectfully submit that the transmission of a sum of the checksums does not teach, describe or suggest "enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets" (emphasis added) as claimed.

Second, Applicants respectfully submit that Miller also teaches away from "enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets" (emphasis added) as claimed.

As understood by the Applicants, Miller discloses a non-repudiation system in which the contents of messages are verified using a cryptographic hash function (col. 2, lines 18-57). Miller recites that "[r]eliability in the Netscape SSL protocol is provided by a common hash function that is applied by a sender to the contents of each outgoing packet and by a receiver to the contents of each incoming packet" (emphasis added; col. 1, lines 28-31). Moreover, in a second embodiment, Miller recites

> The hash values computed by the first entity include a first outgoing hash value that represents the accumulated total of the hash function applied to each of the messages in the first stream since the start position and a first incoming hash value that represents the accumulated total of the hash function applied to each of the messages in the second stream received by the first entity since said start position. The hash values computed by the second entity include a second outgoing hash value representing the accumulated total of the hash function applied to each of the messages in the second stream since the start position and a second incoming hash value representing the accumulated total of the hash function applied to each of the messages in the first stream received by the second entity since the start position. (emphasis added)

Accordingly, Applicants understand Miller to disclose computing hash values for entire messages, and accumulating these hash values.

Therefore, Applicants respectfully submit that Miller does not teach, describe or suggest "calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums" (emphasis added) as claimed. Moreover, by disclosing that a hash value is computed for an entire message, Applicants respectfully submit that Miller teaches away from the claimed embodiments.

Third, Applicants respectfully submit that Miller does not disclose that to which it is asserted as teaching. Specifically, the instant Office Action recites that "Miller discloses calculating a cryptographic checksum for said plurality of data segments (col. 1 lines 27-44)" (emphasis added; instant Office Action; page 4, lines 16-17). In contrast, Miller specifically recites "[o]ther prior art systems provide similar reliability checks by applying the well-known parity, checksum and CRC (cyclic redundancy checking) functions to the outgoing and incoming messages" (emphasis added; col. 1, lines 38-41). Moreover, Miller goes on to recite "[w]hile the Netscape SSL provides secure and reliable network communications, it and many other prior art network security systems do not provide a general property of non-repudiation" (emphasis added; col. 1, lines 41-45).

In particular, Applicants understand Miller to disclose the use of a non-cryptographic checksum, in that the recited checksum does not provide for non-repudiation. Therefore, Applicants respectfully submit that Miller does not disclose a cryptographic checksum as claimed.

Fourth, Applicants respectfully assert that the relied upon disclosures of Miller, (1) the non-cryptographic checksum recited in the Background of the Invention section (col. 1, lines 28-45) and (2) the cryptographic hash of the described invention (at least col. 2, line 35, through col. 3, line 33), are mutually exclusive, and that there is no teaching or suggestion to modify either of the disclosures in the manner suggested in the Office Action.

As presented above, Applicants understand Miller to disclose the use of a non-cryptographic checksum, in that the recited checksum does not provide for non-repudiation.

In contrast, the described invention of Miller describes the use of a cryptographic hash function. Applicants respectfully submit that by explicitly disclosing the shortcoming of prior art systems including checksums as not providing non-repudiation, and by disclosing the cryptographic hash function as overcoming this shortcoming, that there is no teaching, suggestion or motivation within Miller to modify either of the different disclosures in the manner suggested in the instant Office Action, and that these disclosures are mutually exclusive.

Fifth, Applicants respectfully submit that there is no motivation to combine the teachings of Kang and Miller, because Kang teaches away from the suggested modification and modifying Kang as suggested would render Kang unsatisfactory for its intended purpose. Applicants respectfully submit that "[i]t is improper to combine references where the references teach away from their combination" (emphasis added; MPEP 2145(X)(D)(2); *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983)). Applicants respectfully note that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention" (emphasis in original; MPEP 2141.02(VI); *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984)). Moreover, Applicants note that "[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious" (emphasis added) (MPEP 2143.01; *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)). Moreover, "[i]f the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then

there is no suggestion or motivation to make the proposed amendment" (emphasis added) (MPEP 2143.01; *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

As presented above, Applicants respectfully submit that Kang discloses that packet checksums for each packet are included in each packet. In particular, Applicants respectfully submit that it is the intended purpose of Kang to include checksums for each packets with that packet. In contrast, by disclosing that a hash value is computed for an entire message, Applicants respectfully submit that Miller teaches away from the proposed combination with Kang, as this would render Kang unsatisfactory for its intended purpose.

In view of the combination of Wee in view of Kang, further in view of Miller not satisfying the requirements of a *prima facie* case of obviousness, Appellants respectfully submit that independent Claims 1, 23, 27, 29 and 32 overcome the rejection under 35 U.S.C. § 103(a), and that these claims are thus in a condition for allowance. Appellants respectfully submit the combination of Wee in view of Kang, further in view of Miller also does not teach or suggest the additional claimed features of the present invention as recited in Claims 2, 5-10, 12 and 13 that depend from independent Claim 1, Claims 24-26 that depend from independent Claim 23, Claim 28 that depends from independent Claim 27, Claim 30 that depends from independent Claim 29, and Claims 33 and 34 that depend from independent Claim 32. Therefore, Appellants respectfully submit that Claims 2, 5-10, 12, 13, 24-26, 28, 30, 33 and 34 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

3. Whether Claims 11, 14, 15 and 18-22 are unpatentable under 35 U.S.C. §103(a) by Wee in view of Kang, further in view of Miller, yet further in view of Doyle.

The instant Office Action states that Claims 11, 14 ,15 and 18-22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wee in view of Kang, further in view of Miller, yet further in view of Doyle. The Applicants have reviewed Wee, Kang, Miller and Doyle and respectfully submit that the embodiments recited in Claims 11, 14 ,15 and 18-22 are patentable over the combination of Wee, Kang, Miller and Doyle, for at least the following rationale.

Claim 11 is dependent on independent Claim 1 and includes the recitations of Claim 1. Hence, by demonstrating that Wee, Miller, Kang and Doyle do not show or suggest the limitations of independent Claim 1, it is also demonstrated that Wee, Miller, Kang and Doyle do not show or suggest the embodiment of Claim 11.

As presented above, Applicants respectfully submit that the combination of Wee, Kang and Miller does not teach, describe or suggest the recitations of independent Claim 1. Furthermore, Applicants respectfully submit that the combination of Wee, Kang and Miller does not teach, describe or suggest the similar recitations of independent Claim 14.

In particular, as presented above, Applicants respectfully submit that both Kang and Miller teaches away from "enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets" (emphasis added) as claimed. Applicants also respectfully submit that Miller does not disclose that to which it is asserted as teaching. Moreover, Applicants respectfully submit that there is no motivation to combine the teachings of Kang and Miller, because Kang teaches away from the

suggested modification, and modifying Kang as suggested would render Kang unsatisfactory for its intended purpose.

Applicants respectfully submit that Doyle does not overcome the shortcomings of the combination of Wee, Kang and Miller. As understood by the Applicants, Doyle discloses a technique for continuous user authentication. In particular, Applicants respectfully submit that Doyle also does not teach, describe or suggest "calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums" as claimed. In particular, Applicants respectfully submit that Doyle is silent to such a teaching.

Therefore, Applicants respectfully submit that Doyle shares at least some of the shortcomings of Wee, Kang and Miller. Thus, Doyle, alone or in combination with Wee, Kang and/or Miller, does not show or suggest the embodiments as claimed.

In view of the combination of Wee in view of Kang, further in view of Miller, yet further in view of Doyle, not satisfying the requirements of a *prima facie* case of obviousness, Appellants respectfully submit that independent Claims 1 and 14 overcome the rejection under 35 U.S.C. § 103(a), and that these claims are thus in a condition for allowance. Appellants respectfully submit the combination of Wee in view of Kang, further in view of Miller, yet further in view of Doyle, also does not teach or suggest the additional claimed features of the present invention as recited in Claim 11that depends from independent Claim 1 and Claims 15 and 18-22 that depend from independent Claim 14. Therefore, Appellants

respectfully submit that Claims 11, 15 and 18-22 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

Conclusion

Appellants believe that pending Claims 1, 14 and 23 satisfy the requirements of 35 U.S.C. § 112, second paragraph, and that Claims 1, 2, 5-15, 18-30 and 32-34 are patentable over the asserted art under 35 U.S.C. § 103(a). As such, Appellants respectfully request that the rejections of Claims 1, 2, 5-15, 18-30 and 32-34 be reversed.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,
WAGNER BLECHER LLP

Dated: December 1, 2008

/John P. Wagner, Jr./
John P. Wagner, Jr.
Registration No. 35,398
123 Westridge Drive
Watsonville, CA 95076

Phone: (408) 377-0500
Facsimile: (831) 722-2350

VIII. Appendix - Clean Copy of Claims on Appeal

1. A method for ensuring the integrity of data, comprising:

for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums, wherein said plurality of first data segments have a different priority than said plurality of second data segments; and

enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

2. The method described in claim 1 further comprising:

calculating cryptographic checksums for said plurality of said second data segments; and

enabling said cryptographic checksums for said plurality of said second data segments to be transmitted separately from said plurality of data packets.

5. The method described in claim 1 wherein said calculating of said cryptographic checksums utilizes an opportunistic integrity checking scheme.

6. The method described in claim 1 wherein said calculating of said cryptographic checksums is performed using a technique selected from the group consisting of:

a hash function providing a fingerprint of data contained in an encrypted data packet and which guarantees the authenticity of received data and the validity of decrypted data, Message Authentication Codes (MAC), Message Digest algorithms, keyed hashes, SHA

(Secure Hash Algorithm), RIPEMD (RACE Integrity Primitives Evaluation Message Digest), HMAC (keyed-Hashing for Message Authentication), and digital signature schemes.

7. The method described in claim 1 wherein said plurality of said data packets comprises secure scalably streamable data.

8. The method described in claim 1 wherein said plurality of said data packets include data comprising scalably compressed data for media selected from the group consisting of:

speech, audio, image, video, and computer graphics.

9. The method described in claim 1 wherein said plurality of said data packets include data scalably formatted according to techniques selected from the group consisting of:

JPEG-2000 with spatial, frequency, SNR (amplitude), region of interest, or color plane scalability; MPEG-1/2/4 or H.261/2/3/4 using spatial, temporal, or SNR (amplitude), region of interest (ROI) or object scalability or fine-grain scalability (FGS); scalable advanced audio coding (scalable AAC); object-based audio coding using MPEG-4 synthetic audio for individual compression and composition of multiple audio objects; and progressive/scalable graphics compression.

10. The method described in claim 1 wherein said plurality of said data packets comprises media data.

11. The method described in claim 1 wherein said data is stored in a storage medium.

12. The method described in claim 1 further comprising:

encrypting one or more of said data packets.

13. The method described in claim 1 further comprising:

encrypting said cryptographic checksums.

14. A computer readable medium having instructions stored therein for implementing a method for ensuring integrity of data, comprising:

for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums, wherein said plurality of first data segments have a different priority than said plurality of second data segments; and

enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of said data packets.

15. The computer readable medium described in claim 14 wherein said instructions further comprise:

calculating cryptographic checksums for said plurality of said second data segments; and

enabling said cryptographic checksums for said plurality of said second data segments to be transmitted separately from said plurality of said data packets.

18. The computer readable medium described in claim 14 wherein said data packets comprise secure scalably streamable data.

19. The computer readable medium described in claim 14 wherein said data packets comprise media data.

20. The computer readable medium described in claim 14 wherein said data is stored in a storage medium.

21. The computer readable medium described in claim 14 wherein said instructions further comprise:

encrypting one or more of said data packets.

22. The computer readable medium described in claim 14 wherein said instructions further comprise:

encrypting said cryptographic checksums.

23. An apparatus for ensuring integrity of data, comprising:

a receiver for receiving a first plurality of data packets and a second plurality of data packets, each of said packets comprising a plurality of data segments, wherein data segments of said plurality of first data packets have a different priority than data segments of said plurality of second data packets;

a cryptographic checksum calculator coupled to said receiver, said cryptographic checksum calculator for calculating a cryptographic checksum for each of said data segments; and

a cryptographic checksum appender coupled to said cryptographic checksum calculator for assembling said cryptographic checksum.

24. The apparatus described in claim 23 wherein said cryptographic checksum calculator is enabled to

for a plurality of data packets comprising said plurality of first data segments and said plurality of second data segments, calculate a cryptographic checksum for said plurality of said first data segments; and

to enable said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

25. The apparatus described in claim 24 wherein said cryptographic checksum calculator is enabled to calculate said cryptographic checksum for said set of said data segments independently of cryptographic checksums calculated for other sets of said data segments.

26. The apparatus described in claim 23, further comprising a forwarder for forwarding said packets to a destination.

27. A method for ensuring integrity of data, comprising:

receiving a data packet comprising an amount of data partitioned into a plurality of data segments;

calculating a cryptographic checksum for each of a first of said plurality of data segments, wherein said first of said plurality of data segments has a different priority than at least a second of said plurality of data segments; and

enabling said cryptographic checksum for each of said first of said plurality of data segments to be transmitted separately from said data packet.

28. The method described in claim 27 further comprising:

calculating a second cryptographic checksum, wherein a second cryptographic checksum is computed for said second of said plurality of data segments, said first of said plurality of data segments, and said cryptographic checksum for said first of said plurality of data segments.

29. A method for ensuring integrity of data, comprising:

receiving a data packet comprising an amount of data partitioned into at least a plurality of first data segments and a second data segment, wherein said plurality of first data segments has a different priority than said second data segment;

calculating a cryptographic checksum for each of said plurality of first data segments; and

enabling said cryptographic checksums for each of said plurality of first data segments to be transmitted separately from said data packet.

30. The method described in claim 29 further comprising: calculating a second cryptographic checksum for said second data segment; and enabling said cryptographic checksum for said second data segment to be transmitted separately from said data packet.

32. An apparatus for verifying the integrity of data, said apparatus comprising:

a receiver, said receiver configured to receive first data packet, second data packet, and a previously determined cryptographic checksum packet corresponding to said first data packet, wherein said cryptographic checksum packet comprises a plurality of cryptographic checksum associated with said first data packet, wherein said first data packet has a different priority than said second data packet; and

an integrity check module coupled to said receiver, said integrity check module configured to calculate a new cryptographic checksum corresponding to said received first data and to determine whether said new cryptographic checksum matches said previously determined cryptographic checksum.

33. The apparatus of claim 32 wherein said integrity check module is integral with said receiver.

34. The apparatus of claim 32 further comprising:

an output coupled to said integrity check module, said output configured to provide an indication of whether said new cryptographic checksum matches said previously determined cryptographic checksum.

IX. Evidence Appendix

None. No evidence is herein appended.

X. Related Proceedings Appendix

None. No related proceedings are herein appended.